Exhibit C

KrebsonSecurity
In-depth security news and investigation

Ubiquiti Developer Charged With Extortion, Causing 2020 “Breach”

December 2, 2021 48 Comments

In January 2021, technology vendor **Ubiquiti Inc.** [NYSE:UI] disclosed that a breach at a third party cloud provider had exposed customer account credentials. In March, a Ubiquiti employee warned that the company had drastically understated the scope of the incident, and that the third-party cloud provider claim was a fabrication. On Wednesday, a former Ubiquiti developer was arrested and charged with stealing data and trying to extort his employer while pretending to be a whistleblower.

Federal prosecutors say **Nickolas Sharp**, a senior developer at Ubiquiti, actually caused the “breach” that forced Ubiquiti to disclose a cybersecurity incident in January. They allege that in late December 2020, Sharp applied for a job at another technology company, and then abused his privileged access to Ubiquiti’s systems at Amazon’s AWS cloud service and the company’s GitHub accounts to download large amounts of proprietary data.

Sharp’s indictment doesn’t specify how much data he allegedly downloaded, but it says some of the downloads took hours, and that he cloned approximately 155 Ubiquiti data repositories via multiple downloads over nearly two weeks.

On Dec. 28, other Ubiquiti employees spotted the unusual downloads, which had leveraged internal company credentials and a **Surfshark VPN** connection to hide the downloader's true Internet address. Assuming an external attacker had breached its security, Ubiquiti quickly launched an investigation.

But Sharp was a member of the team doing the forensic investigation, the indictment alleges.

"At the time the defendant was part of a team working to assess the scope and damage caused by the incident and remediate its effects, all while concealing his role in committing the incident," wrote prosecutors with the Southern District of New York.

According to the indictment, on January 7 a senior Ubiquiti employee received a ransom email. The message was sent through an IP address associated with the same Surfshark VPN. The ransom message warned that internal Ubiquiti data had been stolen, and that the information would not be used or published online as long as Ubiquiti agreed to pay 25 Bitcoin.

The ransom email also offered to identify a purportedly still unblocked "backdoor" used by the attacker for the sum of another 25 Bitcoin (the total amount requested was equivalent to approximately $1.9 million at the time). Ubiquiti did not pay the ransom demands.

Investigators say they were able to tie the downloads to Sharp and his work-issued laptop because his Internet connection briefly failed on several occasions while he was downloading the Ubiquiti data. Those outages were enough to prevent Sharp's Surfshark VPN connection from functioning properly — thus exposing his Internet address as the source of the downloads.

When FBI agents raided Sharp's residence on Mar. 24, he reportedly maintained his innocence and told agents someone else must have used his Paypal account to purchase the Surfshark VPN subscription.

Several days after the FBI executed its search warrant, Sharp "caused false or misleading news stories to be published about the incident," prosecutors say. Among the claims made in those news stories was that Ubiquiti had neglected to keep access logs that would allow the company to understand the full scope of the intrusion. In reality, the indictment alleges, Sharp had shortened to one day the amount of time Ubiquiti's systems kept certain logs of user activity in AWS.

"Following the publication of these articles, between Tuesday, March 30, 2021 and Wednesday March 31, [Ubiquiti's] stock price fell approximately 20 percent, losing over four billion dollars in market capitalization," the indictment states.

Sharp faces four criminal counts, including wire fraud, intentionally damaging protected computers, transmission of interstate communications with intent to extort, and making false statements to the FBI.

News of Sharp's arrest was first reported by BleepingComputer, which wrote that while the Justice Department didn't name Sharp's employer in its press release or indictment, all of the details align

with previous reporting on the Ubiquiti incident and information presented in Sharp's LinkedIn account. A link to the indictment is here (PDF).

This entry was posted on Thursday 2nd of December 2021 11:11 AM

A LITTLE SUNSHINE | NICKOLAS SHARP | SURFSHARK | UBIQUITI

48 thoughts on "Ubiquiti Developer Charged With Extortion, Causing 2020 "Breach""

Jackson s

December 2, 2021

whoops… got the first report wrong

Nelson Minar

December 2, 2021

Was Sharp the whistleblower source "Adam" in your previous reporting? Because if so you have a journalistic mess to sort out. https://krebsonsecurity.com/2021/04/ubiquiti-all-but-confirms-breach-response-iniquity/

Taylor

December 2, 2021

This is the same Ubiquiti that encourages/requires people to manage their home networks using the Ubiquiti cloud portal.

Lsuoma

-

December 2, 2021

@Taylor – yep, the very same one. Although, it's only the initial config that REQUIRES cloud portal access.

TP Link has a system called Omada which looks pretty good, apart from the APs which a frickin' ugly.

an_n

-

December 3, 2021

You can run standalone on the TP-link also, there's no requirement to use Omada or register.

James Ford

-

December 2, 2021

What's that have to do with this incident, especially since an employee did it from the inside, not the outside?

Taylor

-

December 2, 2021

An employee could sell access to home network administration to the highest bidder. All those home file servers subject to ransomware attack.

This case demonstrates that encouraging people to administer their home networks via a Web portal is criminally irresponsible, and is very likely a class action lawsuit waiting to happen.

Pragdog

-

December 2, 2021

“Criminally irresponsible”?
In ANY country you have a lot to learn about the law. No one has forced you to purchase Ubiquiti equipment and no one is responsible for your choice of vendors but…you. You can register once, set up your new Unifi equipment of choice, disable remote access and access it all locally. Problem solved. No one has external access – and if they do, guess what? It was your own misconfiguration that caused it.

- notIgnorant

-

December 3, 2021

well said !

Matt B

-

December 3, 2021

They do encourage but it’s not mandatory, you can install the management software locally and run it, I’ve run Unifi for years and never touched their cloud services.

However I won’t be touching it again come upgrade time, this being an insider attack does not really change their complete lack of control over their customers data, I’m sure they’re far from the only ones but frankly it’s just not good enough these days.

This one will be a good example of insider attack and why logging/monitoring is critical for years to come.

Seth black

-

December 5, 2021

The engineered obsolescence did not discourage you? Shelving the eol ap expecting a cert break is not a silver lining

Lsuoma

December 2, 2021

His IP leaked when the VPN went down? This is basic OpSec failure. Anyone doing something dodgy that doesn’t use a VPN that kills the connection when it goes down deserves to get caught.

PostToaster

-

December 2, 2021

They deserve to get caught anyway.

Bill Edwards

-

December 3, 2021

Absolutely untrue.

Garn

-

December 2, 2021

The “Kill Switch”

Phil

-

December 6, 2021

Actually, anyone at all deserves to get reprimanded for being ignorant of what a quality VPN should be capable of at bare minimum. This is not just a lesson for the dodgy or even for the consumer, but also for the ‘experts’ who claim to know how to code with failsafe as the core principle, yet fail to test that concept in the real world

The mistake goes like this: Failure analysis/ ‘we will not fail(because we make 6 digits)’/ all systems go…

Randall

December 2, 2021

Factually correct… but I don’t see you taking any responsibility as being the source of misinformation spread by Nikolas Sharp.

https://krebsonsecurity.com/2021/04/ubiquiti-all-but-confirms-breach-response-iniquity/

Matt

-

December 2, 2021

Krebs reported what the source said. Krebs is not the source. I think the readers need to look at themselves and why they believed a single anonymous whistleblower over the official announcements without corroborating evidence one way or the other.

Steve

December 2, 2021

I can see why, under other circumstances, there might not be a statement regarding your source on the insider info from the previous article… but in this case, unless you confirmed that the source’s identity as a particular Ubiquiti employee other than the indicted person, you probably need to reconsider the balance of obligations to your source and your readers. Even the most generous interpretation of omitting a statement on the source is still a head-scratcher. It’s not like

the source's statement was technically wrong, even if it might be really misleading, but I don't think it's unreasonable to just point that out in the piece above the fold.

staylor

-

December 2, 2021

I can see why it could be hard for a reporter to out a confidential source when everything makes a 180 turn. Krebs is probably walking a thin line trying to honor his word to keep the sources name confidential.If your a reporter and it gets around you throw your sources under the bus when things get rough who is going to trust you in the future? Maybe if the guy pleads guilty maybe we can get more details

Evan Hoke

December 2, 2021

whoops… got the first report wrong are you going to update this article to indicate that you didnt fact check properly?

Surf

December 2, 2021

Sounds like SurfShark will give up your account information if it is requested. Pass.

- BrianKrebs Post author

-

December 2, 2021

Preface: I don't know the first thing about Surfshark. But many VPNs will leak your IP under a large number of circumstances that actually are not that infrequent. Having an internet outage causes your VPN to not be able to connect to the internet, like the rest of your connection. The trouble is, unless your VPN client is set to block all traffic if something like this happens, your connection will come back before your VPN does, and any web sockets or connections you had open when your internet connection died may try to reconnect to that site or destination.

That is just one of the many ways IPs can leak through VPNs. Anyway, some of the most popular VPN providers will follow legal process if served by the FBI.

- J

-

December 3, 2021

Hence, the saying " if they pester you with frequent ADS and claim world renowned tech to improve privacy then be certain they're all just current FADS". However there are some respectable vpns that I vouch for such as Mullvad,Proton and IVPN. They operate differently imo and transparent.

bigp

-

December 3, 2021

I think the IP leakage comes from client-side configuration… a fallback if the VPN is down.

Ali

-

December 5, 2021

Proton readily gives access to authorities on their email service so I wouldn't be trusting them with a Vpn no matter how fancy it looks, this info si readily available on the net, been with TorGuard for years, you don't get any dodgy dealings with them, there killswitch just works, they don't mess about when it comes to security.

Liz

December 2, 2021

Nothing shocks me any more, but it is troubling when a developer allegedly abuses his access to perpetrate crimes that cause so much havoc. There is some satisfaction that a technological glitch (VPN) ended up outing him.

I respectfully disagree with some posts urging Krebs to confirm (positive or negative) whether this developer was the source of the earlier article. Sharp has been charged with criminal acts but not convicted yet. There is a long legal and ethical tradition in the U.S. that people are presumed innocent until proved guilty. Last time I checked, we are still bound by that. Even if Sharp was the source and Krebs decided a confirmation would add to the discourse and transparency, it would be premature for Krebs to confirm until Sharp is convicted. Also, if Sharp was the source of the information, it's possible that there are ongoing investigations that require Krebs to keep mum.

People are too quick to criticize and pass judgment. That causes both tangible and intangible damage. Let's all try to be more measured and create a thoughtful space before we react. "Between stimulus and response there is a space. In that space is our power to choose our response. In our response lies our growth and our freedom." — Viktor E. Frankl

Let's also try to remember all the important information that Krebs has brought to his readers before casting that stone.

I'm adding my voice to staylor's post above.

JamminJ

-

December 3, 2021

Well said

Kevin Brown-Goebeler

-

December 8, 2021

My concern is why a developer, even a lead developer, had access to change the logging in the first place. Right to read the logs OK yes that os reasonable. Right to modify, ABSOLUTELY not. And that access fault lies with Ubiquiti not properly managing privileged user access.

Jjjj

December 2, 2021

I am trying to think of what Ubilqiiti is going to do to you specifically Krebs. You personally are responsible for billons of market cap hit

If you haven't already done so, I suggest seeking legal counsel

an_n

-

December 3, 2021

There isn't anything they can do unless 1, he's lying and 2, it's malicious. It is neither. They can write nastygrams all day long in lawyerly fonts but it goes nowhere.

Liz

December 2, 2021

Jjjj

Your comment comes across as a serious allegation against Krebs. I hope you can support your statement with material facts and knowledge of our libel and tort laws.

Freedom of the press is protected by the First Amendment to our Constitution. "In New York Times Co. v. Sullivan, the [Supreme] Court held that proof of actual malice is required for an award of damages in an action for libel involving public officials or matters of public concern. See New York Times Co. v. Sullivan, 376 U.S. 254 (1964). The Court reasoned that speech related to matters of public concern is at the heart of the protections guaranteed by the First Amendment, and outweighs the State's interest in compensating individuals for damage to their reputations. This 'actual malice' test created a national judicial standard for whether speech qualifies as libel." https://www.law.cornell.edu/wex/libel

Ubiquiti is a public traded company and its business is of public concern. Also truth is an absolute defense against defamation. In his earlier article Krebs presented both sides — the charges about the breach made by his unnamed source and Ubiquiti's response to those charges. As far as I can tell, Krebs truthfully reported both sides.

I hasten to add that I am not an attorney but, Jjjj, your allegation that Krebs is personally responsible for financial loss could be viewed by some as being defamatory. You probably meant to be helpful to Krebs and did not intend malice but whether you did may ultimately be in the eye of the beholder.

- BrianKrebs Post author

-

December 3, 2021

As I said on Twitter yesterday, read the March story and then read the government indictment. The only thing that seems to be in dispute is who did it. And my March story didn't touch on the who.

Jay

December 3, 2021

Do any of you readers realize the irony in this? Let me elaborate, 1. Given his position at Company-1, one would assume that he would be aware of what Brian Krebs precisely mentioned above and would plan accordingly just in case. 2. That being said, out of the plethora of VPN's out there this individual that is quite up there earning big $$$ at a tech firm decided to use surf (without reading terms & conditions LMAO) and used a paypal account which was the incriminating factor when the FBI raided the Sharp residence. Simply could have used a VPN that accepts crypto and doesn't required signing up etc which is lower cost btw (25$ he spent lol)

and could have generated more than 1 account and decrease latency to speed up the process of downloading. Truly ironic that you move up the ladder to the point greed overtakes commonsense.

Liz

-

December 4, 2021

I agree. Ironic. I'm reminded of The Peter Principle — that people tend to rise to their level of incompetence. And hubris is fertile grounds for careless errors. There's poetic justice in what led to his arrest.

Seth black

-

December 5, 2021

Using vpn from home ip address is similarly problematic

zyzz

December 3, 2021

He would've been caught even if he hadn't disconnected and leaked. Grabbing the AWS key on his residential IP and two minutes later connecting with Surfshark to use the same key? Nevermind netdata analysis (eg. Team Cymru)/Surfshark cooperating with feds. Very lazy and stupid of him to try and ransom his own employer.

Greg

December 3, 2021

Who gave a developer access to prod in the first place?

JustAnotherGreyBeard

-

December 3, 2021

This. That is "criminally irresponsible."

Steve

-

December 7, 2021

DevOps

Laura

-

December 15, 2021

Who puts stuff in prod, producers?

The Sunshine State

December 3, 2021

Yet another narcissistic loser who didn't practice good OPSEC , especially coming from a intelligent guy who formally worked at Ubiquiti Inc. Where's the irony here ?

Next article please !

John

December 5, 2021

Why do people keep assuming everyone who bought or use any VPN service (that's on the market) they actually use it with their respective apps?
I for instance don't use the official Surfshark client. I use the windows in-built IKEv2 and the browser extension, and those don't have any kill switch (mystery solved)

And yes I understand your point of view (native killswitch not working) but after you saw that article you came here like…. by reading what someone wrote, you know everything and you're entitled to throw BS at this company.

Make your research before accusing someone for something otherwise you are just a sad person with nothing else to do…..

Michael No

December 5, 2021

Now.. typically, Ubiquiti probably hires by focusing on stupid little interview algorithms, instead of focusing on finding truthful and honest developers, backed with true credentials. Go ahead, make hiring stupid so you get stupid people.

- Will S

-

December 9, 2021

BOOM

Integrity is not Taught in College nor online…it is a valuable Character Trait that has cost them…..Billions in lost Revenue as well as Market Share.

THOMAS CALDWELL III

-

December 16, 2021

well said!

Tom Ames

-

December 27, 2021

OK, smart guy: what "true credentials" do YOU PERSONALLY USE to determine that a prospective employee is not going to do something criminal in the future?

This kind of after the fact criticism is just uninformed supposition from someone who clearly has never been a hiring manager.

Reggie

December 19, 2021

Thanks for the information

Comments are closed.